

### **REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed March 24, 2005. Claims 1-17 were pending in the Application. In the Office Action, Claims 1-17 were rejected. Claims 1-17 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

### **SPECIFICATION OBJECTIONS**

The Examiner objected to the disclosure of the specification and requested that serial numbers of co-pending applications be inserted therein. Applicants have so amended the specification to provide the serial numbers of the indicated co-pending applications. Applicants respectfully request that this objection now be withdrawn.

### **SECTION 103 REJECTIONS**

Claims 1-17 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*") in view of U.S. Patent No. 6,134,664 issued to Walker (hereinafter "*Walker*"). Applicants respectfully traverse this rejection.

Of the rejected claims, Claims 1, 8 and 13 are independent. Applicants respectfully submit that neither *Vaidya* nor *Walker*, alone or in combination, discloses, teaches or suggests the limitations of independent Claims 1, 8 and 13.

Independent Claim 1 recites, at least in part, "an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field." Applicants respectfully remind the Examiner that the burden for proving obviousness under 35 U.S.C. § 103 is on the Examiner, and it is the Examiner who has to prove that a

claim is not patentable. In rejecting independent Claim 1 (and remaining Claims 8-17), the Examiner has not provided sufficient reasoning or made any assertions as to why he believes that the portions of at least *Vaidya* referred to by the Examiner disclose particular limitations of Claim 1. The Examiner merely recites Applicants' claim limitation(s) followed by a general recitation of column and line numbers of *Vaidya*, leaving Applicants guessing as to the Examiner's intended meaning. For example, with respect to Applicants' Claim 1 recitation of "an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application," the Examiner merely states "(Col 6, Lines 11-18 and Col 7, Lines 12-24)" (Office Action, page 3) without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach, for example, "an operating system," "a network stack," "a protocol driver," "a media access control driver" or "an intrusion protection system management application" as recited by Claim 1. Further, for example, with respect to Applicants' Claim 1 recitation of "the management application operable to receive text-file input from an input device," the Examiner merely states "(Col 7, lines 24-36, and Col 6, Lines 53-56)" (Office Action, page 3) without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach, for example, "text-file input" or "an input device" as recited by Claim 1. Because the Office Action fails to provide any indication of which components of *Vaidya* are relied upon by the Examiner to teach the limitations of Claim 1, Applicants find it difficult, if not impossible, to adequately address the Examiner's rejection. Applicants request the Examiner to clearly indicate which components of *Vaidya* the Examiner is relying on to teach the limitations of Claim 1 so that Applicants may have a fair opportunity to address the Examiner's concerns.

Regardless, Applicants submit that *Vaidya* does not disclose or even suggest the limitations of independent Claim 1. For example, independent Claim 1 recites "an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application" where "the management application [is] operable to receive text-file input from an input device." The portions of *Vaidya* referred to by the Examiner fail to disclose or even suggest at least

these limitation(s) recited by independent Claim 1, and Applicants are unable to determine why the Examiner believes that the portions of *Vaidya* referred to by the Examiner purportedly teach at least these limitation(s). Applicants respectfully submit that such details are lacking in *Vaidya*, and the Office Action fails to explain why the Examiner believes that such details are present in *Vaidya*. As just one example, Applicants submit that *Vaidya* does not teach or even suggest “text-file input” where the “text-file defin[es] a network-exploit rule” as recited by Claim 1 (emphasis added). Further, *Walker* does not remedy at least this deficiency of *Vaidya*. Therefore, for at least this reason, Applicants submit that Claim 1 is patentable over the cited references.

Moreover, Applicants respectfully submit that there is no motivation or suggestion for combining reference teachings as proposed by the Examiner. For example, independent Claim 1 recites “the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field.” The Examiner admits that *Vaidya* does not disclose a text-file input comprising at least one field (Office Action, page 3), but the Examiner states that *Walker* discloses such limitation and that it would have been obvious to modify *Vaidya* to use signature files comprising at least one field (Office Action, page 3). Applicants respectfully disagree.

*Walker* appears to be directed toward a system for reducing the volume of audit data that is to be evaluated by an intrusion detection system (*Walker*, Abstract, column 4, lines 37-40). *Walker* appears to indicate that such audit data, in the form of an audit trail record, for example, “comprises a plurality of fields” (*Walker*, column 11, lines 29-35). Based on the foregoing, the Examiner appears to arbitrarily import such field into a signature file (“it would [have] been obvious . . . to modify [the] *Vaidya* system to use signature files comprising at least one field”) (Office Action, page 3). Applicants respectfully disagree. The “field” referred to by *Walker* is in an audit trail record and not part of a signature file. Accordingly, neither *Walker* nor *Vaidya*, alone or in combination, suggests including such “field” in a signature file as proposed by the Examiner. Moreover, the Examiner’s basis for including such “field” in a signature file as proposed by the Examiner appears to stem from

the fact that an audit trail record as disclosed by *Walker* includes a “field.” However, *Vaidya* does not appear to disclose or even suggest that any data analyzed by the *Vaidya* system contains any such “fields” that would require that a signature file compared therewith would also require a “field,” nor has the Examiner explicitly identified any such disclosure or suggestion in *Vaidya*. To the contrary, the audit records containing the “field” appear to be limited to the *Walker* reference. Moreover, in support of the Examiner’s reasoning for combining reference teachings, the Examiner states:

One would be motivated to do so in order to enable the system to identify different signatures and take different set[s] of actions for the different signatures to improve the performance of the intrusion detection system.

(Office Action, page 3). Applicants respectfully disagree. The Examiner’s reasoning for including a “field” in a signature file appears to stem from the fact that *Walker* discloses a “field” in an audit record trail. However, the Examiner’s use of such modification as indicated above appears to be independent of whether the data to be compared against such signature field has a “field.” To the contrary, the Examiner’s proposed combination appears to require at least two different steps, neither of which are disclosed or even suggested by the cited references: 1) modifying a signature with a “field” apparently based on the fact that data to be compared with such signature includes a “field;” but 2) using such “field” in the signature file for purposes of identifying different signatures, which appears to be completely independent of whether the data packet in *Vaidya* to be compared against a signature file contains a “field.” Clearly, the Examiner’s bases for combining the reference teachings is unsupported and the Examiner is using hindsight reasoning to piece together the teachings of the cited references to arrive at Applicants’ claimed invention, which is improper. Therefore, for at least this reason also, the rejection of independent Claim 1 is improper and should be withdrawn.

Independent Claim 8 recites “generating a text-file defining a network-exploit rule” and “specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.” At least for the

reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that the rejection of Claim 8 is improper and should be withdrawn. For example, Examiner has not provided sufficient reasoning or made any assertions as to why he believes that the portions of at least *Vaidya* referred to by the Examiner disclose particular limitations of Claim 8. As noted previously, the Examiner merely recites Applicants' claim limitation(s) followed by a general recitation of column and line numbers of *Vaidya*. For example, with respect to Applicants' Claim 8 recitation of "generating a text-file defining a network-exploit rule," the Examiner merely states "(Col 5, Lines 33-39; Col 5, Lines 51-63 and Col 6, Lines 44-56)" (Office Action, page 6) without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach, for example, "generating a text-file" or a text-file that "defin[es] a network-exploit rule" as recited by Claim 8. To the contrary, Applicants respectfully submit that *Vaidya* does not disclose or even suggest such limitation(s), nor does Walker remedy at least this deficiency of *Vaidya*. Accordingly, for at least this reason, Applicants respectfully submit that the rejection of Claim 8 is improper.

Further, Claim 8 recites "specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file." The Examiner admits that *Vaidya* does not disclose this limitation(s) (Office Action, page 6), but the Examiner states that *Walker* teaches such limitation and that it would have been obvious to modify *Vaidya* to use signature files comprising at least one field (Office Action, pages 6-7). Applicants respectfully disagree. As discussed above in connection with independent Claim 1, Applicants submit that there is no motivation or suggestion to combine reference teachings as suggested by the Examiner based solely on an audit trail record having a "field" (as disclosed by *Walker*). Further, the Examiner appears to completely ignore various limitations of Claim 8. For example, *Walker* does not appear to disclose or even suggest "specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file" as recited by Claim 8 (emphasis added), nor has the Examiner explicitly identified any such disclosure in *Walker*. In fact, the Examiner does not even refer to this limitation(s) in the

Examiner's reference to *Walker*. Accordingly, for at least this reason also, the rejection of Claim 8 is improper and should be withdrawn.

Independent Claim 13 recites "reading input from an input device of the computer," "compiling the input into a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field," "evaluating the machine-readable signature file" and "determining the value of the at least one field of the machine-readable signature file." For at least the reasons discussed above in connection with independent Claim 1 and 8, Applicants respectfully submit that the rejection of Claim 13 is improper. For example, as stated above, the Examiner merely refers generally to various portions of *Vaidya* as purportedly teaching the limitations of Claim 13 without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach such limitations. Further, even when Applicants assume which components of *Vaidya* the Examiner may be referring to as purportedly teaching the limitations of Claim 13, the portions of *Vaidya* referenced by the Examiner are insufficient. For example, the Examiner refers to column 5, lines 51-63, of *Vaidya* as teaching "reading input from an input device of the computer" and "compiling the input into a machine-readable signature file" as recited by Claim 13. Applicants disagree. Column 5, lines 51-63, of *Vaidya* recite the following:

A configuration generator 28 is connected to the database handler to enable the network administrator to define the configuration of network objects on the LAN 11 and the remote network 24. The configuration generator 28 also enables the administrator to define the connection of both the LAN 11 and the remote network 24 to the Internet. Network objects include devices such as . . . [and] further include applications and files stored in memory within those devices. Based on the network configuration data generated by the configuration generator 28, the database handler 26 assigns sets of attack signatures profiles to each data collector 10.

Thus, the portion referred to by the Examiner appears to disclose that for a particular network object of *Vaidya*, a particular set of signature profiles will be used to analyze data packets directed to that particular network object (see also column 6, lines 1-15, of *Vaidya*).

Accordingly, *Vaidya* does not disclose or even suggest, in the portion referred to by the Examiner or elsewhere in *Vaidya*, “reading input from an input device of the computer” and “compiling the input into a machine-readable signature file” as recited by Claim 13. Moreover, *Walker* does not appear to remedy at least these deficiencies of *Vaidya*.

Further, as discussed above, Applicants submit that there is no motivation or suggestion to combine reference teachings as suggested by the Examiner based solely on an audit trail “field” as suggested by the Examiner. Additionally, Claim 13 recites “a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field” (emphasis added). The Examiner appears to ignore at least these limitation(s) because the Examiner does not appear to even refer to these limitation(s) in the Examiner’s reference to Claim 13 and/or *Walker*. Accordingly, for at least these reasons, the rejection of Claim 13 is improper.

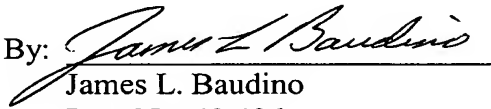
Claims 2-7, 9-12 and 14-17 depend respectively from independent Claims 1, 8 and 13. For at least the reasons discussed above, Claims 1, 8 and 13 are in condition for allowance and, therefore, Claims 2-7, 9-12 and 14-17 that depend respectively therefrom are also in condition for allowance. Accordingly, Applicants respectfully requests that the rejection of Claims 2-7, 9-12 and 14-17 be withdrawn.

**CONCLUSION**

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicant has overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By:   
James L. Baudino  
Reg. No. 43,486

Date: June 22, 2005

Correspondence to:  
L.Joy Griebenow  
Hewlett-Packard Company  
Intellectual Property Administration  
P. O. Box 272400  
Fort Collins, CO 80527-2400  
Tel. 970-898-3884